United States General Accounting Office

GAO

Report to the Secretary of the Treasury

August 1999

BUREAU OF THE PUBLIC DEBT

Areas for Improvement in Computer Controls

GAO/AIMD-99-242

GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, D.C. 20548

Accounting and Information
Management Division

B-283207

August 6, 1999

The Honorable Lawrence H. Summers
The Secretary of the Treasury

Dear Mr. Secretary:

In connection with fulfilling our requirement to audit the U.S. government's fiscal year 1998 financial statements, we audited and reported on the Bureau of the Public Debt's (BPD) Schedules of Federal Debt Managed by BPD for the fiscal years ended September 30, 1998 and 1997 (GAO/AIMD-99-70). Our review of the general and application computer controls over key BPD financial systems was performed as part of these audits. On July 16, 1999, we issued a "Limited Official Use" report to you detailing the results of our review. This excerpted version of the report for public release summarizes the vulnerabilities we identified and the recommendations we made.

This report discusses the results of our tests of the effectiveness of general and application controls that support key BPD automated financial systems and our follow-up on the status of BPD's corrective actions to address vulnerabilities identified in our fiscal year 1997 audit. These systems, some of which are operated and maintained by the Federal Reserve Banks (FRB), process investments in and redemption of Treasury securities, generate interest payments, account for the resulting federal debt, and provide financial reports to the public and the federal government. We also assessed the general and application controls over key BPD systems that the FRBs maintain and operate and will be issuing a separate report to the Board of Governors of the Federal Reserve System on the results of our testing.

As we reported in connection with our audit of the Schedules of Federal Debt, the management of BPD fairly stated that its internal control, including computer controls, was effective. In that report, we did not identify any reportable conditions.[1] However, as discussed in this report,

[1]Reportable conditions are matters coming to our attention that, in our judgement, should be communicated because they represent significant deficiencies in the design or operation of internal control that could adversely affect the organization's ability to meet the objective of reliable financial reporting and compliance with applicable laws and regulations.

we identified vulnerabilities involving general and application computer controls that we did not consider reportable conditions but, if left uncorrected, increase the risk of inappropriate disclosure or modification of sensitive information or disruption of critical operations. These vulnerabilities warrant BPD management's attention and action. In light of the significant reliance on interconnected electronic data and automated systems to support program operations and to replace manual procedures and paper documents, well-designed and properly implemented general and application controls are essential to protect BPD's computer resources and ensure continuity of operations. While performing our work, we communicated detailed information regarding our findings to BPD management. This report provides an overall assessment of BPD's computer control vulnerabilities and summarizes those findings.

Results in Brief

Our follow-up on the status of BPD's corrective actions to address vulnerabilities identified in our fiscal year 1997 audit found that BPD had corrected or mitigated the risks associated with 13 of the 21 general and application control vulnerabilities discussed in our prior report.[2] Our fiscal year 1998 audit procedures identified certain new general control vulnerabilities in access controls, system software controls, and application software development and change controls. We also identified vulnerabilities in the controls for two key BPD financial applications maintained and operated at the BPD data center in Parkersburg, West Virginia, involving authorization, completeness, and accuracy controls.

Overall, we found that BPD general and application controls combined with other management and manual reconciliation controls were effective in ensuring BPD's ability to report reliable financial information and data. Although various management and reconciliation controls help BPD detect potential irregularities or improprieties in its financial data or transactions, these types of compensating controls do not prevent certain threats to its computer resources and operating environment from unintentional errors or omissions or intentional modification, disclosure, or destruction of data and programs by disgruntled employees, intruders, or hackers. Thus, the vulnerabilities we noted increase the risks of inappropriate disclosure and modification of sensitive data and programs, misuse or damage of computer resources, or disruption of critical operations. BPD informed us

[2] Bureau of the Public Debt: Areas for Improvement in Computer Controls (GAO/AIMD-99-2, October 14, 1998).

that it agreed with our findings and that in most cases, it had corrected or is in the process of correcting the vulnerabilities that we identified.

Background

The Department of the Treasury is authorized by the Congress to borrow money on the credit of the United States to fund operations of the federal government. Within Treasury, BPD is responsible for prescribing the debt instruments, limiting and restricting the amount and composition of the debt, paying interest to investors, and accounting for the resulting debt. In addition, BPD has been given responsibility for issuing Treasury securities to trust funds for trust fund receipts not needed for current benefits and expenses.

As of September 30, 1998 and 1997, federal debt managed by BPD totaled about $5.5 trillion and $5.4 trillion, respectively, for monies borrowed to fund the government's operations. These balances consisted of (1) $3.8 trillion as of September 30, 1998 and 1997, owed to the public and (2) $1.7 trillion as of September 30, 1998, and $1.6 trillion as of September 30, 1997, owed to federal entities, such as the Social Security Trust funds. Total interest expense for fiscal years 1998 and 1997 was $363 billion and $356 billion, respectively.

BPD relies on a number of interconnected financial systems and electronic data to process and track the money that is borrowed and to account for the securities it issues. The FRBs also provide fiscal agent services on behalf of BPD, which primarily consist of issuance, servicing, and redemption of Treasury securities; processing secondary market transactions; and handling the related transfers of funds. The FRBs use a number of financial systems to process debt-related transactions throughout the country. Detailed data initially processed at the FRBs are summarized and then forwarded electronically to BPD's Parkersburg, West Virginia, data center for matching, verification, and posting to the general ledger.

Objectives, Scope, and Methodology

Our objectives were to evaluate and test the effectiveness of the controls over key financial management systems maintained and operated by BPD and to determine the status of the computer control vulnerabilities identified in our fiscal year 1997 audit. Using a rotation approach for testing general controls, the scope of our work for fiscal year 1998 included

follow-up on vulnerabilities identified in our prior year report and the following three general controls areas intended to

- protect data and application programs from unauthorized access, modification, and destruction;
- prevent the introduction of unauthorized changes to application and system software; and
- ensure recovery of computer processing operations in case of a disaster or other unexpected interruption.

To evaluate these general controls, we identified and reviewed BPD's information system general control policies and procedures, conducted tests and observations of controls in operation, and held discussions with officials at the BPD data center to determine whether controls were in place, adequately designed, and operating effectively. Our penetration testing was expanded over the prior year to include internal penetration testing procedures. Through our internal and external penetration testing, we attempted to access sensitive data and programs. These attempts were performed with the knowledge and cooperation of BPD officials.

We also used a rotation approach to evaluate controls over selected applications. We performed a full-scope application controls review of one key financial application to determine whether the application is designed to ensure that

- access privileges establish individual accountability and proper segregation of duties, limit the processing privileges of individuals, and prevent and detect inappropriate or unauthorized activities;
- data are authorized, converted to an automated form, and entered into the application accurately, completely, and timely;
- data are properly processed by the computer and files are updated correctly;
- erroneous data are captured, reported, investigated, and corrected; and
- files and reports generated by the application represent transactions that actually occur and accurately reflect the results of processing, and reports are controlled and distributed to the authorized users.

The scope of our work over another key financial application included follow-up on vulnerabilities that we identified in our fiscal year 1997 audit and focused on the application's accuracy control area, which is designed to ensure that erroneous data are captured, reported, investigated, and corrected.

Because the FRBs are integral to the operations of BPD, we followed up on the status of the FRB's corrective actions to address vulnerabilities identified in our fiscal year 1997 audit.[3] We assessed the general controls over BPD systems that the FRBs maintain and operate. We also evaluated application controls over three key BPD financial applications maintained and operated by the FRBs.

To assist in our evaluation and testing of computer controls, we contracted with the independent public accounting firm PricewaterhouseCoopers LLP. We determined the scope of our contractor's audit work, monitored its progress, and reviewed the related work papers to ensure that the resulting findings were adequately supported.

During the course of our work, we communicated our findings to BPD management who informed us that BPD has taken or plans to take corrective action to address the vulnerabilities we identified. We plan to follow up on these matters during our audit of the U.S. government's fiscal year 1999 financial statements.

We performed our work at the BPD data center in Parkersburg, West Virginia, from September 1998 through January 1999. Our work was performed in accordance with generally accepted government auditing standards. We requested comments on a draft of this report from the Department of the Treasury. Its comments are discussed in the "Agency Comments" section of this report.

Areas for Improvement in BPD's General Computer Controls

General controls are the structure, policies, and procedures that apply to an entity's overall computer operations. General controls establish the environment in which application systems and controls operate. They include an entitywide security program, access controls, system software controls, application software development and change controls, segregation of duties, and service continuity controls. An effective general control environment would (1) ensure that an adequate computer security planning and management program is in place, (2) protect data, files, and programs from unauthorized access, modification, and destruction, (3) limit and monitor access to programs and files that control computer hardware and secure applications, (4) prevent unauthorized programs or

[3] Federal Reserve Banks: Areas for Improvement in Computer Controls (GAO/AIMD-99-6, October 14, 1998).

unauthorized changes to existing programs from being implemented, (5) prevent any one individual from controlling key aspects of computer-related operations, and (6) ensure the recovery of computer processing operations in case of a disaster or other unexpected interruption.

We identified vulnerabilities in access controls, system software controls, application software development and change controls, and service continuity controls. These vulnerabilities, if left uncorrected, increase the risk of inappropriate disclosure or modification of sensitive data and programs or disruption of critical operations.

Access Controls

Access controls are designed to limit or detect access to computer programs, data, equipment, and facilities to protect these resources from unauthorized modification, disclosure, loss, or impairment. Such controls include logical and physical security controls.

Logical security control measures involve the use of computer hardware and software to prevent or detect unauthorized access by requiring users to input unique user identifications (ID), passwords, or other identifiers that are linked to predetermined access privileges. Logical security controls restrict the access of legitimate users to the specific systems, programs, and files they need to conduct their work and prevent unauthorized users from gaining access to computing resources.

We found internal network access control vulnerabilities that expose BPD systems to the risk of unauthorized access to systems, sensitive data, and computing resources. While a disgruntled employee or unintentional error or omission could disrupt BPD's operations, the segregation of responsibilities between BPD and the FRBs and the transmission from the FRBs of only summary-level information to BPD adequately prevent one individual from completing a debt-related transaction. Other key management and manual reconciliation controls at BPD help to detect irregularities or improprieties in its financial data or transactions. These controls include (1) extensive background investigations on all employees, (2) management monitoring and review of assigned workloads, exception reports, and end-of-day unauthorized transactions exception reports, and (3) daily independent manual and automated reconciliations of Treasury debt security issuance, redemption, and interest payment transactions with the applicable FRBs and the Treasury's Financial Management Service Funds Control Branch. Due to the sensitive nature of the internal network

control vulnerabilities we identified, these issues are described in the separate "Limited Official Use" report issued to you on July 16, 1999.

Physical security controls include locks, guards, badges, alarms, and similar measures (used alone or in combination) that help to safeguard computer facilities and resources from intentional or unintentional loss or impairment by limiting access to the buildings and rooms where they are housed.

The BPD Network Operations Branch (NOB) issues card-keys to grant approved individuals access to the data center. During our review, we noted that NOB's informal procedures for requesting and approving access to the data center are not consistently enforced. For card-keys issued to 152 individuals by the NOB data center, we noted the following.

- Seven employees were provided card-keys without completing a card-key access request form.
- One card-key access request form was not signed and approved by the NOB manager.
- In 34 instances, card-key access request forms contained multiple employees although BPD's policies require card-key access request forms be prepared for each individual.
- Twenty of the card-key access request forms did not contain the employees' job titles.
- One card-key access request form was incomplete and did not list the correct user department.

Incomplete or unapproved card-key access forms increase the risk that individuals who were not granted explicit access privileges could gain unauthorized or inappropriate command center card-key access.

System Software

System software coordinates and helps control the input, processing, output, and data storage associated with all of the applications that run on a system. System software include operating system software, system utilities, program library systems, file maintenance software, security software, data communications systems, and database management systems. Controls over access to and modification of system software are essential to protect the overall integrity and reliability of information systems.

We found that a production library, which houses the files containing the sequence of instructions for performing particular tasks, such as linking programs, databases, and files needed to execute transactions, contained library members that are no longer needed or used. We also noted that management review and approval is not required in the existing process used to identify obsolete object code contained in library members. Inadvertent or intentional use of the obsolete object code from unused production library members could disrupt operations or cause unexpected financial reporting results. The risk of potential irregularities or improprieties in BPD's financial data is mitigated by its independent manual and automated reconciliation controls, but these do not eliminate the potential for disruption of operations.

Application Software Development and Change Controls

Controls over the design, development, and modification of application software help to ensure that all programs and program modifications are properly authorized, tested, and approved. Such controls also help prevent security features from being inadvertently or deliberately turned off and processing irregularities or malicious code from being introduced.

During our review of BPD's application software development and change control processes, we found the following.

- The users and their supporting application developers for five BPD applications did not consistently follow Treasury or BPD application software development and change control guidelines. Specifically, of the 16 change control items judgmentally selected for testing, we found the following.
  - Updates to the Functional Requirements Document, Detailed Design Document, and User Training Manual were not made for each of the four application enhancement change items selected for testing. Of the remaining 12 change items selected for testing, programmer comments in the software code were not included for 5 program changes. Failure to consistently update and maintain pertinent documents and user manuals increases the risk of programming or user mistakes and inefficiencies.
  - Written approval to move software change items from the acceptance region to the production region was not obtained for 5 of the 16 change items. Consequently, the risk of unauthorized introduction and execution of program modifications is increased.
  - Written evidence of user acceptance test plans or test results was not maintained for 4 of the 16 change items. Undocumented user

acceptance test plans and results increase the risk of inadequate testing, which could result in the introduction and execution of unauthorized changes.

- A contributing factor to the findings described above is that the Treasury's Information System Life Cycle and the BPD Application Systems Division Handbook do not contain standard practices that require (1) written authorization to move application software from the acceptance region to the production region and (2) retention guidelines for user acceptance test plans and results.
- BPD also uses several change and problem management tools to manage software changes, user change requests, and software problem reporting. Summary-level monitoring reports have to be manually compiled from the four software change tracking tools used by BPD rather than systematically from a single source. As such, the efficiency with which BPD resources may be deployed is decreased.

To a certain extent, BPD's low turnover and extensive in-house knowledge reduce the risk that knowledge of the applications could be lost or application maintenance could become inefficient. However, these factors do not replace the benefits of a well-designed and managed application software development and change control process to prevent unintentional or intentional programming errors or omissions.

Service Continuity

An organization's ability to accomplish its mission can be significantly affected if it loses the ability to process, retrieve, and protect information that is maintained electronically. For this reason, organizations should have (1) established procedures for protecting information resources and minimizing the risk of unplanned interruptions and (2) plans for recovering critical operations should interruptions occur. A contingency or disaster recovery plan specifies emergency response, backup operations, and postdisaster recovery procedures to ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation. It addresses how an organization will deal with a full range of contingencies, from electrical power failures to catastrophic events, such as earthquakes, floods, and fires. The plan also identifies essential business functions and ranks resources in order of criticality. To be most effective, a contingency plan should be periodically tested in disaster simulation exercises and employees should be trained in and familiar with its use.

In reviewing BPD's service continuity and contingency planning, we found that corrective actions had not been completed for the vulnerabilities we identified in our prior year audit related to (1) the close proximity of the offsite storage, (2) contingency plan testing, and (3) the adequacy of the backup power supply.

The limited contingency plan testing conducted to date provides some level of assurance to certain components of its disaster recovery plan. However, events such as changes to BPD's computing environment (including hardware, software, networks, procedures, and personnel) increase the risk that BPD may not be prepared to effectively prioritize recovery activities, integrate recovery steps in an effective manner, or fully recover systems during an actual emergency.

BPD's Application Controls Can Be Strengthened

Application controls relate directly to the individual computer programs that are used to perform certain types of work, such as generating interest payments or recording transactions in a general ledger. In an effective general control environment, application controls ensure that transactions are valid, properly authorized, and completely and accurately processed and reported.

In addition to testing general controls, we tested application controls for two key financial applications and identified vulnerabilities in authorization, completeness, and accuracy controls.

Authorization Controls

Like general access controls, authorization controls for specific applications should be established to ensure individual accountability and proper segregation of duties, ensure that only authorized transactions are entered into the application and processed by the computer, limit the processing privileges of individuals, and prevent and detect inappropriate or unauthorized activities.

As we previously reported in our fiscal year 1997 audit, we identified instances where access to one of the tested application's functions and/or data was not adequately controlled or documented. Specifically,

- although their job responsibilities do not require such access rights, BPD staff members responsible for the application's support have routine rather than emergency-only access to functions that allow them to enter transactions and

- policies and procedures for performing changes to the application's master data have not been formally documented in writing, increasing the risk that unauthorized changes could be made.

Completeness Controls

Completeness controls are designed to ensure that all transactions are processed and missing transactions are identified. Common completeness controls include the use of record counts and control totals, computer sequence checking, computer matching of transaction data with data in a master or suspense file, and checking of reports for transaction data.

We found that certain interface files developed by BPD for one of the applications do not contain trailer records with record counts or control totals because it is not a requirement of BPD's software design policy. In addition, certain of these interface files did not contain header records. Without automated controls such as header and trailer records with record counts and control totals, there is an increased risk that incomplete financial information or transactions could be transmitted and not promptly detected resulting in a misstatement in financial or other data. BPD relies on manual detection and monthly reconciliation controls to ensure files are successfully received and transactions are processed and reported. However, these manual controls do not replace the efficiencies gained by using automated control procedures that are performed on a real-time basis to identify and prevent the transmission of incomplete, erroneous, or fraudulent data.

Accuracy Controls

The recording of valid and accurate data into application systems is essential to an effective system that produces reliable results. Accuracy controls include (1) well-designed data entry processes, (2) data validation and editing to identify erroneous data, (3) reporting, investigating, and correcting erroneous data, and (4) review and reconciliation of output.

We previously reported in our fiscal year 1997 audit that BPD uses a powerful software utility to delete one of the tested application's exception reports from the production databases. During our fiscal year 1998 audit, we found that BPD continues to use the powerful software utility to delete exception reports because corrections to the application have not been fully completed and implemented. Although BPD has developed informal procedures for using the powerful software utility, the privileges provided by the utility go far beyond those needed by an individual to perform his or her job responsibilities. Consequently, there is the risk that an individual

could use the more powerful features of the software utility to deliberately or inadvertently delete critical production data operations.

During the year, the introduction of a new application improved the processing cycle times for recording savings bond transactions from 6 weeks to 3 days. This application allowed BPD to report transfer matching errors on a more timely basis. However, BPD had not revised its procedures by increasing the frequency of its exception report review to respond to the significant reduction in processing cycle times. Consequently, matching errors will not be corrected in a timely manner.

FRB Computer Controls Can Be Improved

Our follow-up work found that the FRBs had corrected many of the vulnerabilities that were identified in our prior year report and that work is in progress to address the remaining vulnerabilities. Our fiscal year 1998 audit procedures identified vulnerabilities in general controls that do not have a significant adverse impact on the BPD financial systems, but nonetheless warrant FRB management's attention and action. These include vulnerabilities in general controls over (1) entitywide security program, (2) access to data, programs, and computing resources, (3) application software development and change controls, (4) segregation of duties, and (5) service continuity. We also found vulnerabilities in authorization controls over one application. We are providing details of these matters in a separate report to the Board of Governors of the Federal Reserve System along with our recommendations for improvement. FRB management has informed us that the FRBs have taken or plan to take corrective actions to address the vulnerabilities we identified. We plan to follow up on these matters during our audit of the U.S. government's fiscal year 1999 financial statements.

Conclusion

Well-designed and properly implemented general and application controls are essential to protect BPD's computer resources and operational environment from the risks of inappropriate disclosure and modification of sensitive information, misuse or damage of computer resources, and disruption of critical operations. BPD needs to take preventive measures to further reduce its exposure to certain threats to its computer resources and operating environment due to unintentional errors or omissions, or intentional modification, disclosure, or destruction of data and programs by disgruntled employees, intruders, or hackers. As we noted, BPD has addressed most of the vulnerabilities we identified as part of our fiscal year

1997 audit. For fiscal year 1998, BPD has already taken some actions to resolve the new vulnerabilities we identified; but further actions are required to fully address the vulnerabilities discussed in this report.

Recommendations

In our July 16, 1999, "Limited Official Use" version of this report, we recommended that you direct the Commissioner of the Bureau of the Public Debt to take specific actions to correct each of the individual vulnerabilities that were identified during our testing and summarized in that report.

We also recommended that you direct the Commissioner of BPD to work with the FRBs to implement corrective actions to resolve the computer control vulnerabilities related to BPD systems supported by FRBs that we identified and communicated to the FRBs during our testing.

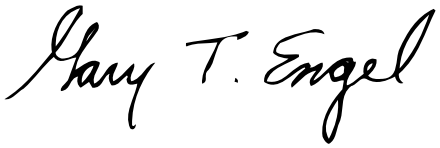
Agency Comments

In commenting on a draft of this report, BPD agreed with our findings. The Commissioner of the Bureau of the Public Debt stated that in most cases, BPD has corrected or is already taking actions to resolve the vulnerabilities identified in the report.

We are sending copies of this report to Senator Robert C. Byrd, Senator Ben Nighthorse Campbell, Senator Pete V. Domenici, Senator Byron L. Dorgan, Senator Frank R. Lautenberg, Senator Joseph Lieberman, Senator Daniel Patrick Moynihan, Senator William V. Roth, Jr., Senator Ted Stevens, and Senator Fred Thompson and to Representative Bill Archer, Representative Dan Burton, Representative Stephen Horn, Representative Steny H. Hoyer, Representative John R. Kasich, Representative Jim Kolbe, Representative Charles B. Rangel, Representative John M. Spratt, Jr., Representative Jim Turner, and Representative Henry A. Waxman in their capacities as Chairmen or Ranking Minority Members of Senate or House Committees and Subcommittees. We are also sending copies of this report to Mr. Van Zeck, Commissioner, Bureau of the Public Debt; the Honorable Jacob Lew, Director, Office of Management and Budget; and Mr. Lawrence W. Rogers, Acting Inspector General, Department of the Treasury. Copies will also be made available to others upon request.

If you have any questions regarding this report, please contact me at (202) 512-3406. Key contributors to this assignment were J. Lawrence Malenich, Paula M. Rascona, and Gregory C. Wilshusen.

Sincerely yours,



Gary T. Engel
Associate Director
Governmentwide Accounting and
Financial Management Issues

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary, VISA and MasterCard credit cards are accepted, also.

Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000 or by using fax number (202) 512-6061, or TDD (202) 512-2537.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web Home Page at:

http://www.gao.gov

PRINTED ON RECYCLED PAPER

United States
General Accounting Office
Washington, D.C. 20548-0001

Official Business
Penalty for Private Use $300

Address Correction Requested

Bulk Rate
Postage & Fees Paid
GAO
Permit No. GI00